



## **Avaya Solution & Interoperability Test Lab**

---

# **Avaya Aura™ SIP Enablement Services Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in a Centralized Trunking Configuration – Issue 1.0**

### **Abstract**

These Application Notes present a sample configuration of the Avaya Aura™ SIP Enablement Services 5.2.1 Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in a Centralized Trunking configuration.

This solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the Avaya SIP call control platform (i.e. Avaya Aura™ SIP Enablement Services) located at the main site is lost. Connectivity loss can be caused by WAN access problems being experienced at the branch or by network problems at the main site blocking access to the Avaya SIP call control platform, or by Avaya Aura™ SIP Enablement Services going out of service.

The Survivable SIP Gateway Solution monitors the connectivity health from the remote branch to the Avaya SIP call control platform at the main site. When connectivity loss is detected, the Avaya one-X™ Deskphone SIP 9600 Series IP Telephones at the branch, as well as the Juniper SRX210 Services Gateway, dynamically switch to Survivability Mode, restoring telephony services to the branch for intra-branch and PSTN calling.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes present a sample configuration of the Avaya Aura™ SIP Enablement Services 5.2.1 Survivable SIP Gateway Solution using the Juniper SRX210 SIP Services Gateway in a Centralized Trunking configuration.

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the SIP call control platform (i.e. Avaya Aura™ SIP Enablement Services) at the main site occurs. Connectivity loss can be caused by WAN access problems being experienced at the branch or by network problems at the main site blocking access to the Avaya SIP call control platform, or by Avaya Aura™ SIP Enablement Services going out of service. The survivable SIP gateway solution monitors connectivity health from the remote branch to the Avaya SIP call control platform at the main site. When connectivity loss is detected, SIP endpoints and SIP gateway components within the branch dynamically switch to survivability mode restoring basic telephony services to the branch for intra-branch and PSTN calling. When connectivity from the branch to the Avaya SIP call control platform at the main site is restored, SIP components in the branch dynamically switch back to normal operations.

The primary components of this solution are the Avaya one-X™ Deskphone SIP 9600 Series IP Telephones, the Juniper SRX210 Services Gateway, Avaya Aura™ Communication Manager, as well as Avaya Aura™ SIP Enablement Services, which provides the centralized SIP control platform with SIP registrar and proxy functions in Normal Mode. The sample configuration shown in these Application Notes utilizes the Juniper Services Gateway model SRX210; however, these configuration steps can also be applied to the Juniper SRX240 Services Gateway using the Juniper firmware version specified in **Section 3**.

## 1.1. Interoperability Testing

The interoperability testing focused on the dynamic switch from Normal Mode (where the network connectivity between the main site and the branch site is intact) to Survivable Mode (where the network connectivity between the main site and the branch site is broken) and vice versa. The testing also verified interoperability between the Avaya 9600 Series SIP Phones and the Juniper SRX210 Services Gateway in Survivable Mode.

### 1.1.1. Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager

The Avaya Aura™ SIP Enablement Services is a routing hub for SIP calls among connected SIP telephony system components. In the test configuration, all Avaya 9600 Series SIP Phones at the central location register to the Avaya Aura™ SIP Enablement Services. All Avaya 9600 Series SIP Phones at the branch site register simultaneously to the Avaya Aura™ SIP Enablement Services at the main location and the Juniper SRX210 Services Gateway at the branch. The Avaya Aura™ SIP Enablement Services provides centralized SIP call control in Normal Mode; the branch Juniper SRX210 provides local SIP control in Survivable Mode. In Normal Mode, the phone calling features are supported by Avaya Aura™ Communication Manager. The Avaya 9600 Series SIP Phones are configured on Communication Manager as Off-PBX-Stations (OPS).

### 1.1.2. Juniper SRX210 Services Gateway

The Juniper SRX210 Services Gateway, referred to as Juniper SRX210 (or SRX210) throughout the remainder of this document, takes on various roles based on call flows and network conditions. The following lists these roles:

- SIP PSTN Media Gateway (FXO / T1 interfaces to PSTN)
- SIP Analog Terminal Adapter (FXS interfaces to analog endpoints)
- SIP Registrar and Proxy (dynamically activated on detection of lost connectivity to the SIP control platform at the main site)
- SIP Trunk Edge Point (acts as a B2BUA to Branch IP Phones and SIP Trunk Providers)

The SRX210 combines routing, security and switching functionality with onboard PoE (Power on Ethernet) to power the Avaya IP Phones. With 1 IP port used for the WAN connection, there are 7 ports remaining for direct connections to branch IP phones and/or other IP devices. The SRX210 also provides 2 FXS ports (for analog phone connections) and 2 FXO ports (for analog line connections to the PSTN).

### 1.1.3. Avaya one-X™ Deskphone SIP 9600 Series IP Telephone

The Avaya one-X™ Deskphone SIP 9600 Series IP Telephone, referred to as Avaya 9600 SIP Phone throughout the remainder of this document, is a key component of the survivable SIP gateway solution. The 2.5 firmware release of the Avaya 9600 SIP Phone tested with the sample configuration includes feature capabilities specific to SIP survivability, enabling the phone to monitor connectivity to Avaya Aura™ SIP Enablement Services and dynamically failover to the local Juniper SRX210 as a survivable SIP server. See reference [5] for additional information on the Avaya 9600 SIP Phone.

### 1.1.4. Network Modes

**Normal Mode:** In Normal Mode, the branch has WAN connectivity to the main site and the Avaya SIP call control platform is being used for all branch calls.

**Survivable Mode:** In Survivable Mode, the branch has lost WAN connectivity to the main site. The local branch Juniper SRX210 is used for all calls at that branch. Note that if the Avaya Aura™ SIP Enablement Services, which provides the centralized SIP call control, loses connectivity to the WAN, all branches will go into Survivable Mode simultaneously.

### 1.1.5. PSTN Trunking Configurations

The Avaya Aura™ SIP Enablement Services Survivable SIP Gateway Solution can interface with the PSTN in either a Centralized Trunking or a Distributed Trunking configuration. These trunking options determine how branch calls to and from the PSTN will be routed over the corporate network. Consider an enterprise consisting of a main Headquarters/Data Center location and multiple branch locations that are all inter-connected over a corporate WAN. The

following descriptions define Centralized Trunking and Distributed Trunking as related to this survivable SIP gateway solution:

**Centralized Trunking:** In Normal Mode, all PSTN calls, inbound to the enterprise and outbound from the enterprise, are routed from/to the PSTN connection configured on the Avaya Media Gateway (located at the main site). In Survivable Mode, PSTN calls to/from the branch phones are routed through the analog trunks from the Service Provider connected to the FXO interface ports on the branch Juniper SRX210 Services Gateway.

**Distributed Trunking:** Outgoing PSTN calls are routed based on ARS analysis on Communication Manager and Host Maps on SIP Enablement Services. Local calls from branch locations are routed back to the same branch location and terminate on the FXO interface of the local Juniper SRX210 Services Gateway. This solution has the potential benefits of saving bandwidth on the branch access network, off-loading the WAN and centralized media gateway resources, avoiding Toll Charges, and reducing latency.

Note that with the sample configuration:

1. In both Normal and Survivable Mode, 911 emergency calls from the branch should always be routed through the FXO interfaces on the branch SRX210 to the local Emergency Response Center (regardless of whether Centralized or Distributed Trunking is being used).
2. In both Centralized Trunking and Distributed Trunking configurations, routing of DID (Direct Inward Dialing) calls from the PSTN to the FXO interfaces on the branch SRX210 is determined by the network mode that the branch is currently operating in:
  - If the branch is in Normal Mode, the DID call will be routed to the Headquarters for further routing decisions. The DID call can terminate either to a Headquarters phone or to a branch phone depending on further digits collected from the calling party.
  - If the branch is in Survivable Mode, the DID call will be terminated to the Auto-Attendant on the SRX210 for onward routing to branch phones on user-provided branch extension numbers.

The two trunking configurations share mostly the same configuration procedures on Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, and the Juniper SRX210. The configuration procedures in this document implement the Centralized Trunking configuration.

## 1.2. Support

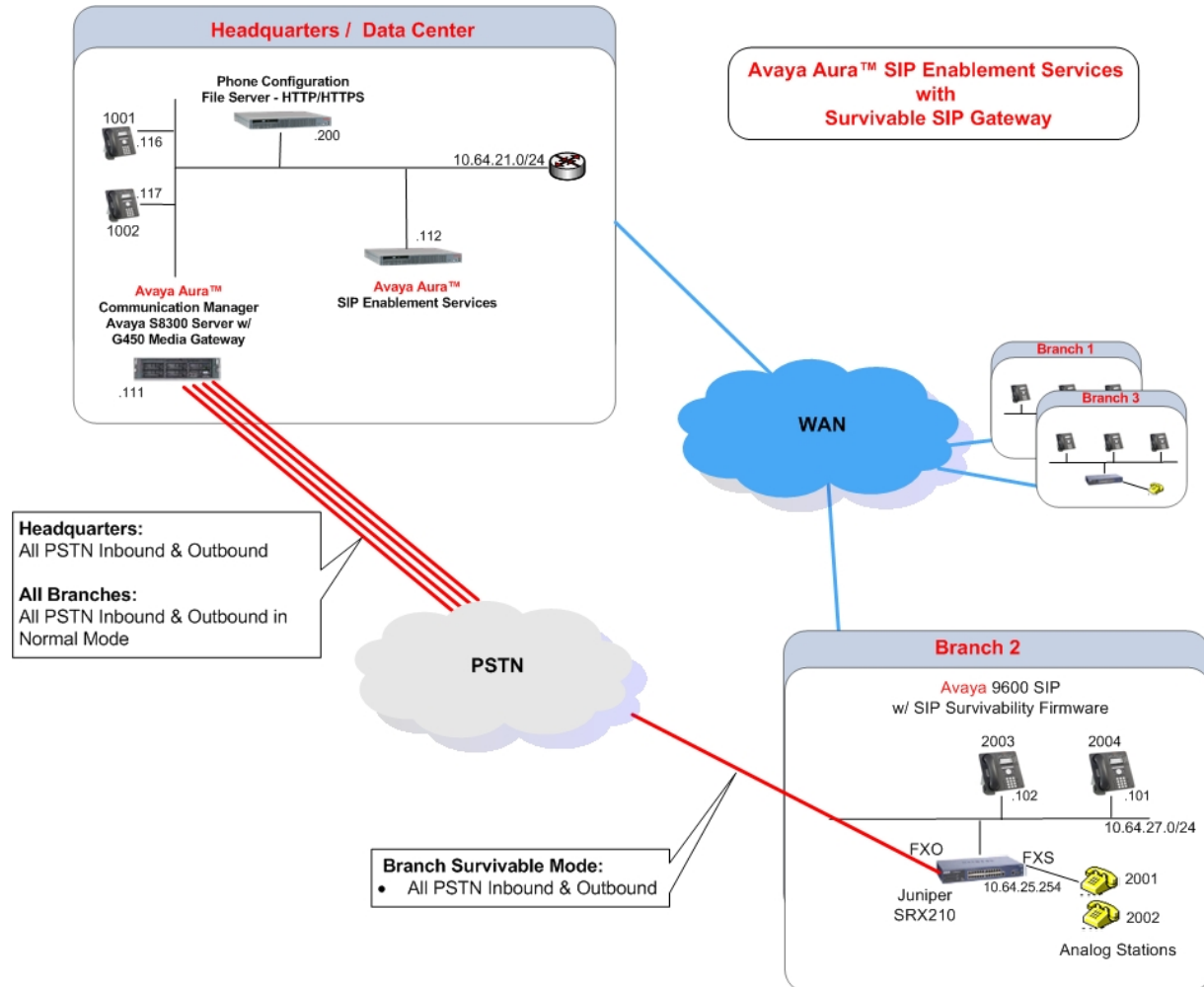
For technical support on the Juniper SRX210, contact Juniper Networks via the support web site <http://www.juniper.net/customers/support>.

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support. Customers may also use specific numbers provided on <http://support.avaya.com> to directly access specific support and consultation services based upon their Avaya support agreements.

## 2. Reference Configuration

The network implemented for the sample configuration shown in **Figure 1** is modeled after an enterprise consisting of a main Headquarters/Data Center location and multiple branch locations all inter-connected over a corporate WAN. One sample branch configuration was documented in the ensuing sections of these Application Notes.

The Headquarters location hosts a SIP Enablement Services server providing enterprise-wide SIP call control, and a Communication Manager providing both advanced feature capabilities to Avaya 9600 SIP Phones, and trunks to the PSTN. Avaya Aura™ Communication Manager Messaging is also located at the Headquarters location to provide the voice mail messaging service (not shown). In addition, the Headquarters location hosts an Avaya IP Phone Configuration File Server for Avaya 9600 SIP Phones to download configuration information. SIP Enablement Services, Communication Manager, and the phone configuration file server are connected to the 10.64.21.0/24 subnet.



**Figure 1 – Network Diagram**

The configuration details of the phone configuration file server as well as Communication Manager Messaging are considered outside the scope of these Application Notes and are therefore not included.

The Avaya IP Phone Configuration File Server contains a 46xxsettings.txt file used by Avaya IP phones to set values of the phone configuration parameters. **Section 6** includes the parameters of the 46xxsettings.txt file used by the Avaya 9600 SIP Phones for survivability. Communication Manager Messaging can be reached by dialing the internal extension configured as the voice mail access number, or by dialing a PSTN number that also terminates to the voice messaging application. The internal extension is configured in the 46xxsettings.txt file as the default voice mail access number to dial when the Message button of the Avaya 9600 SIP Phone is pressed while the phone is in Normal Mode. The external PSTN number is configured in the 46xxsettings.txt file as an alternate voice mail access number to dial when the Message button of the Avaya 9600 SIP Phone is pressed while the branch phone is in Survivable Mode. This enables branch users to continue to access the centralized voice mail service while in Survivable Mode.

The branch locations consist of two Avaya 9600 SIP Phones, a Juniper SRX210 Services Gateway with PSTN analog trunks connected to the FXO interface ports, and two analog phones on the FXS interfaces.

In the sample configuration, all phones at both the main and branch sites are SIP phones (branch analog sets are adapted by the Juniper SRX210 as SIP phones too).

The configuration details throughout this document utilize the network information as listed in **Table 1**.

| IP Network                                      | IP Network<br>Region<br>on<br>Communication<br>Manager | Area Code | Juniper SRX210<br>IP Address   |
|---|--|-----------|--|
| 10.64.21.0/24                                   | 1  | 303       |  |
| 10.64.25.0/24<br>10.64.26.0/24<br>10.64.27.0/24 | 1  | 732       | 10.64.25.254<br>(assigned to port 7<br>to provide<br>connectivity to the<br>WAN) |

**Table 1 – Network Information**

### 3. Equipment and Software Validated

The following components were used for the sample configuration:

| Component   | Software/Firmware   |
|---|---|
| Avaya S8500C Server                                     | Avaya Aura™ SIP Enablement Services 5.2.1                           |
| Avaya S8300 Server in a<br>Avaya G450 Media Gateway     | Avaya Aura™ Communication Manager 5.2.1<br>(R015x.02.1.016.4-17959) |
| Avaya 9600 Series IP Telephones<br>Model: 9620 and 9630 | Avaya one-X™ Deskphone Edition SIP 2.5.0                            |
| Avaya 6210 Analog Telephone                             | -   |
| HTTPS/HTTP Phone<br>Configuration File Server           | Windows Server 2003 SP2   |
| Juniper SRX210  | 10.1-20100504.0   |

**Table 3 – Software/Hardware Version Information**



## 4. Configure Avaya Aura™ Communication Manager

This section shows the necessary steps to configure Communication Manager to support the survivable SIP gateway solution. It is assumed that the basic configuration on Communication Manager, the required licensing, as well as the configuration required for accessing Communication Manager Messaging, has already been administered. See the reference documents in **Section 11** for additional information.

All commands discussed in this section are executed on Communication Manager using the System Access Terminal (SAT).

The administration procedures in this section include the following areas. Some administration screens have been abbreviated for clarity.

- Verify Avaya Aura™ Communication Manager license
- Configure System parameters features
- Configure IP node names
- Configure IP codec set
- Configure IP network regions
- Add Stations
- Configure SIP signaling group and trunk group
- Configure Route pattern
- Configure Public numbering
- Configure Automatic Route Selection (ARS)

#### 4.1. Verify Avaya Aura™ Communication Manger License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum capacities permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

| display system-parameters customer-options                        |           | Page 2 of 11 |
|---|-----------|--------------|
| OPTIONAL FEATURES   |           |              |
| IP PORT CAPACITIES  | USED      |              |
| Maximum Administered H.323 Trunks: 450                            | 12        |              |
| Maximum Concurrently Registered IP Stations: 450                  | 0         |              |
| Maximum Administered Remote Office Trunks: 0                      | 0         |              |
| Maximum Concurrently Registered Remote Office Stations: 0         | 0         |              |
| Maximum Concurrently Registered IP eCons: 0                       | 0         |              |
| Max Concur Registered Unauthenticated H.323 Stations: 50          | 0         |              |
| Maximum Video Capable Stations: 50                                | 0         |              |
| Maximum Video Capable IP Softphones: 50                           | 0         |              |
| <b>Maximum Administered SIP Trunks: 450</b>                       | <b>84</b> |              |
| Maximum Administered Ad-hoc Video Conferencing Ports: 0           | 0         |              |
| Maximum Number of DS1 Boards with Echo Cancellation: 0            | 0         |              |
| Maximum TN2501 VAL Boards: 0                                      | 0         |              |
| Maximum Media Gateway VAL Sources: 20                             | 1         |              |
| Maximum TN2602 Boards with 80 VoIP Channels: 0                    | 0         |              |
| Maximum TN2602 Boards with 320 VoIP Channels: 0                   | 0         |              |
| Maximum Number of Expanded Meet-me Conference Ports: 0            | 0         |              |
| (NOTE: You must logoff & login to effect the permission changes.) |           |              |

## 4.2. Configure System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system-wide basis.

**Note:** This feature poses security risks, and must be used with caution. As an alternative, the trunk-to-trunk transfer feature can be implemented using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in **Section 11** for more details.

```
change system-parameters features                               Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
      Music/Tone on Hold: music Type: ext 68000
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? y
```

## 4.3. Configure IP Node Names

Use the “change node-names ip” command to add an entry for the SIP Enablement Services server that the Communication Manager will connect to. The **Name** “SES” and **IP Address** “10.64.21.112” are entered for SIP Enablement Services. The configured node-name “SES” will be used later in the SIP Signaling Group administration (**Section 4.7.1**).

```
change node-names ip                                           Page 1 of 2
      IP NODE NAMES
      Name      IP Address
      SES       10.64.21.112
      SM        10.64.20.31
      default   0.0.0.0
      msgserver 10.64.21.113
      procr     10.64.21.111
```

## 4.4. Configure IP Codec Set

Configure the IP codec set to use for SIP calls. Use the “change ip-codec-set n” command, where “n” is the codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields.

In the sample configuration, IP codec set 1 was used for the IP network regions assigned to the Headquarters and Branch locations.

|                       |             |         |          |      |      |   |
|-----------------------|-------------|---------|----------|------|------|---|
| change ip-codec-set 1 |             |         |          | Page | 1 of | 2 |
| IP Codec Set          |             |         |          |      |      |   |
| Codec Set: 1          |             |         |          |      |      |   |
| Audio                 | Silence     | Frames  | Packet   |      |      |   |
| Codec                 | Suppression | Per Pkt | Size(ms) |      |      |   |
| 1: G.711MU            | n           | 2       | 20       |      |      |   |
| 2:                    |             |         |          |      |      |   |

## 4.5. Configure IP Network Regions

For simplicity, IP network region 1 was used for the phones and servers at the Headquarters and Branch locations. Other configurations are possible. An IP address map can be used for network region assignment if required.

The **Authoritative Domain** “ses.avaya.com” matches the SIP domain configured in SIP Enablement Services (**Section 5.2**). The **Codec Set** for intra-region calls is set to the codec set “1” as configured in **Section 4.4**. The **IP-IP Direct Audio** parameters retain the default “yes” allowing direct IP media paths both within the region and between regions to minimize the use of media resources in the Avaya Media Gateway.

|                                       |  |  |  |      |      |    |
|---------------------------------------|--|--|--|------|------|----|
| change ip-network-region 1            |  |  |  | Page | 1 of | 19 |
| IP NETWORK REGION                     |  |  |  |      |      |    |
| Region: 1                             |  |  |  |      |      |    |
| Location: 1                           |  |  |  |      |      |    |
| Name: HQ - Avaya Equipment            |  |  |  |      |      |    |
| Authoritative Domain: ses.avaya.com   |  |  |  |      |      |    |
| MEDIA PARAMETERS                      |  |  |  |      |      |    |
| Codec Set: 1                          |  |  |  |      |      |    |
| Intra-region IP-IP Direct Audio: yes  |  |  |  |      |      |    |
| Inter-region IP-IP Direct Audio: yes  |  |  |  |      |      |    |
| UDP Port Min: 2048                    |  |  |  |      |      |    |
| UDP Port Max: 35889                   |  |  |  |      |      |    |
| IP Audio Hairpinning? y               |  |  |  |      |      |    |
| DIFFSERV/TOS PARAMETERS               |  |  |  |      |      |    |
| RTCP Reporting Enabled? y             |  |  |  |      |      |    |
| Call Control PHB Value: 48            |  |  |  |      |      |    |
| RTCP MONITOR SERVER PARAMETERS        |  |  |  |      |      |    |
| Audio PHB Value: 48                   |  |  |  |      |      |    |
| Video PHB Value: 26                   |  |  |  |      |      |    |
| Use Default Server Parameters? y      |  |  |  |      |      |    |
| 802.1P/Q PARAMETERS                   |  |  |  |      |      |    |
| Call Control 802.1p Priority: 6       |  |  |  |      |      |    |
| Audio 802.1p Priority: 6              |  |  |  |      |      |    |
| Video 802.1p Priority: 5              |  |  |  |      |      |    |
| AUDIO RESOURCE RESERVATION PARAMETERS |  |  |  |      |      |    |
| RSVP Enabled? n                       |  |  |  |      |      |    |
| H.323 IP ENDPOINTS                    |  |  |  |      |      |    |
| H.323 Link Bounce Recovery? y         |  |  |  |      |      |    |
| Idle Traffic Interval (sec): 20       |  |  |  |      |      |    |
| Keep-Alive Interval (sec): 5          |  |  |  |      |      |    |
| Keep-Alive Count: 5                   |  |  |  |      |      |    |

## 4.6. Add Stations

A station must be created on Communication Manager for each SIP User account to be created in SIP Enablement Services which includes a provisioned Communication Manager Extension. The extension assigned to the Communication Manager station must match the Communication Manager Extension assignment in SIP Enablement Services (see **Section 5.3.2**).

Use the “add station” command to add a station to Communication Manager. The “add station” command for an Avaya 9620 SIP Phone located in the branch, and assigned to extension 2001, is shown below. Because this is a SIP station, only the **Type** and **Name** fields are required to be populated as highlighted in bold. All remaining fields can be left at default values. Feature programming for each station can vary.

| add station 2001          |                         | Page 1 of 6 |
|---------------------------|-------------------------|-------------|
| STATION                   |                         |             |
| Extension: 2001           | Lock Messages? n        | BCC: 0      |
| <b>Type: 9620SIP</b>      | Security Code: 123456   | TN: 1       |
| Port: S00000              | Coverage Path 1: 1      | COR: 1      |
| <b>Name: FXS 1</b>        | Coverage Path 2:        | COS: 1      |
|                           | Hunt-to Station:        |             |
| STATION OPTIONS           |                         |             |
|                           | Time of Day Lock Table: |             |
| Loss Group: 19            |                         |             |
|                           | Message Lamp Ext: 2001  |             |
| Display Language: english |                         |             |
| Survivable COR: internal  |                         |             |
| Survivable Trunk Dest? y  | IP SoftPhone? n         |             |
|                           | IP Video? n             |             |

On **Page 6** of the station form, specify “8” for **SIP Trunk**. That is the SIP trunk administered in **Section 4.7**.

| add station 2001           |  | Page 6 of 6 |
|----------------------------|--|-------------|
| STATION                    |  |             |
| SIP FEATURE OPTIONS        |  |             |
| Type of 3PCC Enabled: None |  |             |
| <b>SIP Trunk: 8</b>        |  |             |

Repeat the above procedures to add each SIP phone located at both the main site and the branch sites, including the branch analog stations. Note that a phone type of “9620SIP” should be used for the branch analog stations.

After all the stations have been added, use the “list off-pbx-telephone station-mapping” command to verify that all the stations have been automatically designated as OPS (Off-PBX Station) sets. In the screen shown below, extensions 1001 and 1002 are SIP phones at the main site; extensions 2001 and 2002 are analog phones at the branch; and extensions 2003 and 2004 are SIP phones at the branch.

| list off-pbx-telephone station-mapping |      |    |              |               |                 |                 |                  |
|--|------|----|--------------|---------------|-----------------|-----------------|------------------|
| STATION TO OFF-PBX TELEPHONE MAPPING   |      |    |              |               |                 |                 |                  |
| Station<br>Extension                   | Appl | CC | Phone Number | Config<br>Set | Trunk<br>Select | Mapping<br>Mode | Calls<br>Allowed |
| 1001                                   | OPS  |    | 1001         | 1 /           | 8               | both            | all              |
| 1002                                   | OPS  |    | 1002         | 1 /           | 8               | both            | all              |
| 2001                                   | OPS  |    | 2001         | 1 /           | 8               | both            | all              |
| 2002                                   | OPS  |    | 2002         | 1 /           | 8               | both            | all              |
| 2003                                   | OPS  |    | 2003         | 1 /           | 8               | both            | all              |
| 2004                                   | OPS  |    | 2004         | 1 /           | 8               | both            | all              |

## 4.7. Configure SIP Signaling Group and Trunk Group

A SIP signaling group and an associated trunk group was configured between Communication Manager and SIP Enablement Services in the sample configuration. The signaling and trunk groups were used for call signaling and media transport to/from SIP phones registered to SIP Enablement Services including phones in the branch location (when in Normal Mode).

### 4.7.1. SIP Signaling Groups

Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** “procr” node name from **Section 4.3**
- **Far-end Node Name:** “SES” SIP Enablement Services node name from **Section 4.3**
- **Near-end Listen Port:** “5061”
- **Far-end Listen Port:** “5061”
- **Far-end Network Region:** Network region number “1” from **Section 4.5**
- **Far-end Domain:** SIP domain name from **Section 4.5** and **Section 5.2**
- **DTMF over IP:** “rtp-payload”
- **Direct IP-IP Audio Connections:** “y”

```
add signaling-group 8                                     Page 1 of 1
                                                         SIGNALING GROUP

Group Number: 8                      Group Type: sip
                                     Transport Method: tls

IMS Enabled? n
IP Video? n

Near-end Node Name: procr              Far-end Node Name: SES
Near-end Listen Port: 5061             Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: ses.avaya.com

Incoming Dialog Loopbacks: eliminate    Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3      IP Audio Hairpinning? n
Enable Layer 3 Test? n                  Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n  Alternate Route Timer(sec): 6
```

## 4.7.2. SIP Trunk Groups

Use the “add trunk-group n” command, where “n” is an available trunk group number, to add SIP trunk groups. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** Descriptive text
- **TAC:** An available trunk access code as per dial plan
- **Service Type:** “tie”
- **Signaling Group:** The signaling group number as configured in **Section 4.7.1**
- **Number of Members:** Equal to the maximum number of concurrent calls supported

```
add trunk-group 8                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 8                                     Group Type: sip          CDR Reports: y
  Group Name: CM to SES                           COR: 1          TN: 1          TAC: *008
    Direction: two-way                           Outgoing Display? n
    Dial Access? n                               Night Service:
    Queue Length: 0
  Service Type: tie                               Auth Code? n
                                               Signaling Group: 8
                                               Number of Members: 10
```

Navigate to **Page 3**, and enter “public” for the **Numbering Format** field as shown below. Use the default values for all other fields.

```
add trunk-group 8                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                               Measured: none
                                               Maintenance Tests? y
                                               Numbering Format: public
                                               UUI Treatment: service-provider
                                               Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
Show ANSWERED BY on Display? y
```



## 4.8. Configure Route Patterns

Configure a route pattern to route calls through the added SIP trunk group. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name
- **Grp No:** The trunk group number configured in **Section 4.7.2**
- **FRL:** Facility Restriction Level that allows access to this trunk, “0” being the least restrictive

|                        |     |           |     |     |        |     |          |         |                 |  |      |      |                      |      |
|------------------------|-----|-----------|-----|-----|--------|-----|----------|---------|-----------------|--|------|------|----------------------|------|
| change route-pattern 8 |     |           |     |     |        |     |          |         |                 |  |      |      | Page 1 of 3          |      |
| Pattern Number: 8      |     |           |     |     |        |     |          |         |                 |  |      |      | Pattern Name: to SES |      |
| SCCAN? n               |     |           |     |     |        |     |          |         |                 |  |      |      | Secure SIP? n        |      |
| Grp                    | FRL | NPA       | Pfx | Hop | Toll   | No. | Inserted |         |                 |  |      |      | DCS/                 | IXC  |
| No                     |     |           | Mrk | Lmt | List   | Del | Digits   |         |                 |  |      |      | QSIG                 |      |
|                        |     |           |     |     |        |     |          |         |                 |  |      |      | Dgts                 |      |
|                        |     |           |     |     |        |     |          |         |                 |  |      |      | Intw                 |      |
| 1:                     | 8   | 0         |     |     |        |     |          |         |                 |  |      |      | n                    | user |
| 2:                     |     |           |     |     |        |     |          |         |                 |  |      | n    | user                 |      |
| 3:                     |     |           |     |     |        |     |          |         |                 |  |      | n    | user                 |      |
| 4:                     |     |           |     |     |        |     |          |         |                 |  |      | n    | user                 |      |
| 5:                     |     |           |     |     |        |     |          |         |                 |  |      | n    | user                 |      |
| 6:                     |     |           |     |     |        |     |          |         |                 |  |      | n    | user                 |      |
|                        |     |           |     |     |        |     |          |         |                 |  |      |      |                      |      |
|                        |     | BCC VALUE |     | TSC | CA-TSC |     | ITC BCIE |         | Service/Feature |  | PARM | No.  | Numbering            | LAR  |
|                        |     | 0         | 1   | 2   | M      | 4   | W        | Request |                 |  |      | Dgts | Format               |      |
|                        |     |           |     |     |        |     |          |         |                 |  |      |      | Subaddress           |      |
| 1:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |
| 2:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |
| 3:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |
| 4:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |
| 5:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |
| 6:                     | y   | y         | y   | y   | y      | n   | n        | rest    |                 |  |      |      |                      | none |

## 4.9. Configure Public Numbering

Use the “change public-unknown-numbering 0” command to define the calling party number to be sent. Add an entry for the trunk group defined in **Section 4.7.2**. In the example shown below, all calls originating from a 4-digit extension beginning with “1” and routed across trunk group 8 will result in a 4-digit calling number. The calling party number will be in the SIP “From” header.

|                                   |      |        |  |        |  |     |  |                       |  |             |  |
|-----------------------------------|------|--------|--|--------|--|-----|--|-----------------------|--|-------------|--|
| change public-unknown-numbering 0 |      |        |  |        |  |     |  |                       |  | Page 1 of 2 |  |
| NUMBERING - PUBLIC/UNKNOWN FORMAT |      |        |  |        |  |     |  |                       |  |             |  |
| Total                             |      |        |  |        |  |     |  |                       |  |             |  |
| Ext                               | Ext  | Trk    |  | CPN    |  | CPN |  |                       |  |             |  |
| Len                               | Code | Grp(s) |  | Prefix |  | Len |  |                       |  |             |  |
|                                   |      |        |  |        |  |     |  | Total Administered: 2 |  |             |  |
| 4                                 | 1    | 8      |  |        |  | 4   |  | Maximum Entries: 240  |  |             |  |

## 4.10. Configure Automatic Route Selection (ARS)

The ARS entries highlighted in this section focus on the local and long distance dialing from branch locations.

### 4.10.1. ARS Access Code

The sample configuration designates '9' as the ARS Access Code as shown below on **Page 1** of the **change feature-access-codes** form. Calls with a leading 9 will be directed to the ARS routing table.

| change feature-access-codes                          |  | Page 1 of 9    |
|--|--|----------------|
| FEATURE ACCESS CODE (FAC)                            |  |                |
| Abbreviated Dialing List1 Access Code:               |  |                |
| Abbreviated Dialing List2 Access Code:               |  |                |
| Abbreviated Dialing List3 Access Code:               |  |                |
| Abbreviated Dial - Prgm Group List Access Code:      |  |                |
| Announcement Access Code: *09                        |  |                |
| Answer Back Access Code:                             |  |                |
| Attendant Access Code:                               |  |                |
| Auto Alternate Routing (AAR) Access Code: 0          |  |                |
| <b>Auto Route Selection (ARS) - Access Code 1: 9</b> |  | Access Code 2: |
| Automatic Callback Activation:                       |  | Deactivation:  |
| Call Forwarding Activation Busy/DA: All:             |  | Deactivation:  |
| Call Forwarding Enhanced Status: Act:                |  | Deactivation:  |
| Call Park Access Code:                               |  |                |
| Call Pickup Access Code:                             |  |                |
| CAS Remote Hold/Answer Hold-Unhold Access Code:      |  |                |
| CDR Account Code Access Code:                        |  |                |
| Change COR Access Code:                              |  |                |
| Change Coverage Access Code:                         |  |                |
| Conditional Call Extend Activation:                  |  | Deactivation:  |
| Contact Closure Open Code:                           |  | Close Code:    |

### 4.10.2. ARS Digit Analysis

The “change ars analysis y” command is used to make routing entries where the y is the dialed digit string to match. The ARS Digit Analysis Table used in the sample configuration is shown below. Calls to the PSTN with area code 303 (1 + 10 digits) will match the **Dialed String** of “1303” with “11” digits and select **Route Pattern** “3”. Calls to the PSTN with area code “732” will match the **Dialed String** of “173” with “11” digits and also select **Route Pattern** “3”. Note that in a real deployment environment, calls with other area codes or with no area code restrictions (i.e., **Dialed String** “1xxxxxxxxx”) can be specified to fit specific business policies.

|                          |         |         |      |      |      |  |               |   |    |   |
|--------------------------|---------|---------|------|------|------|--|---------------|---|----|---|
| change ars analysis 130  |         |         |      |      |      |  | Page          | 1 | of | 2 |
| ARS DIGIT ANALYSIS TABLE |         |         |      |      |      |  | Percent Full: |   |    |   |
| Location: all            |         |         |      |      |      |  | 0             |   |    |   |
| Dialed                   | Total   | Route   | Call | Node | ANI  |  |               |   |    |   |
| String                   | Min Max | Pattern | Type | Num  | Reqd |  |               |   |    |   |
| 1303                     | 11 11   | 3       | fnpa |      | n    |  |               |   |    |   |

|                          |         |         |      |      |      |  |               |   |    |   |
|--------------------------|---------|---------|------|------|------|--|---------------|---|----|---|
| change ars analysis 173  |         |         |      |      |      |  | Page          | 1 | of | 2 |
| ARS DIGIT ANALYSIS TABLE |         |         |      |      |      |  | Percent Full: |   |    |   |
| Location: all            |         |         |      |      |      |  | 0             |   |    |   |
| Dialed                   | Total   | Route   | Call | Node | ANI  |  |               |   |    |   |
| String                   | Min Max | Pattern | Type | Num  | Reqd |  |               |   |    |   |
| 173                      | 11 11   | 3       | fnpa |      | n    |  |               |   |    |   |

The routing of E-911 calls is outside the scope of these Application notes. However, an ARS Digit Analysis entry should be created to route the E-911 calls to the SIP Enablement Services for onward routing to the PSTN. Routing policies would be defined on the SIP Enablement Services to

- Route E-911 calls originated from the branch in the Normal Mode to go out to the PSTN through the FXO interfaces on the branch Juniper SRX210
- Route E-911 calls originated from the Headquarters to go out to the PSTN through the E1/T1 facilities at the central site

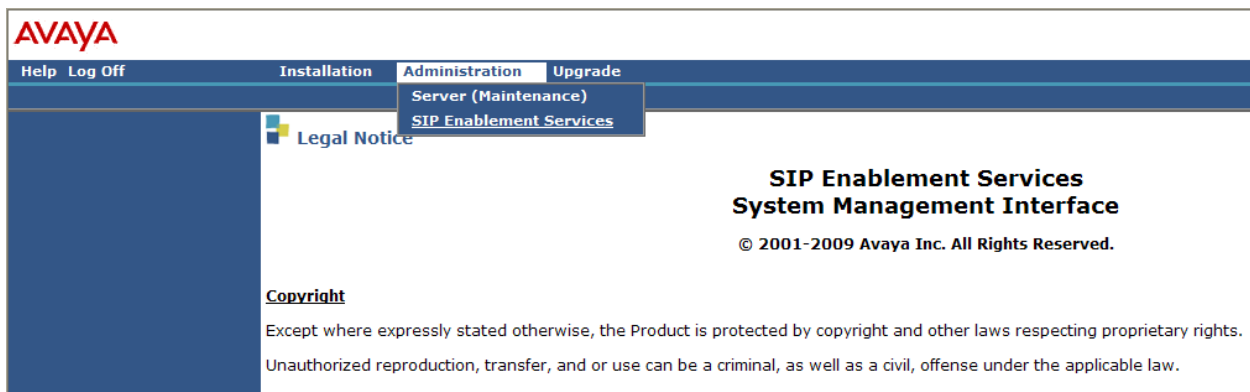
This assures the E-911 calls from both Headquarters and branch sites would be received by the local Emergency Response Center.

## 5. Configure Avaya Aura™ SIP Enablement Services

This section provides the procedures for configuring SIP Enablement Services as provisioned in the sample configuration. SIP Enablement Services is configured via an Internet browser using the administration web interface. It is assumed that the SIP Enablement Services software and the license file have already been installed on the server. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure SIP Enablement Services.


### 5.1. Login

Access the SES administration web interface by entering <https://<ip-addr>/admin> as the URL in an Internet browser, where [<ip-addr>](#) is the IP address of the SIP Enablement Services server. Log in with the appropriate credentials and then navigate to the **Administration → SIP Enablement Services** link from the main page shown below.



## 5.2. System Properties

Administer the SIP domain. Navigate to **Server Configuration → System Properties**. Set SIP Domain to match the Authoritative Domain and Far-end Domain administered on Communication Manager in **Sections 4.5 and 4.7.1**.



Help Exit

Top

Users

Address Map Priorities

Adjunct Systems

Aggregator

Certificate Management

Conferences

Emergency Contacts

Export/Import to ProVision

Hosts

IM logs

Communication Manager Servers

Communication Manager Extensions

Server Configuration


SIP Phone Settings

Survivable Call Processors

System Status

Trace Logger

Trusted Hosts

 **View System Properties**

SES VersionSES-5.2.1.0-016.4

System ConfigurationSimplex

Host TypeSES combined home-edge

SIP Domain\*

Note that the DNS domain is avaya.com

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

SIP License Host\*

**DiffServ/TOS Parameters**

Call Control PHB Value\*

**802.1 Parameters**

Priority Value\*

Management System Access Login

Management System Access Password

DB Log Level

© 2006 Avaya Inc. All Rights Reserved

## 5.3. SIP User Accounts

### 5.3.1. Avaya 9600 SIP Phone Accounts

An account must be created for each Avaya 9600 SIP Phone user (at both the branch and main site) by selecting **User → Add** from the SES left navigation panel. Each user account must also be configured with a Communication Manager Extension. The screen below, left, illustrates the creation a user account for branch SIP phone of the sample configuration.

After adding the user account, the **Add Communication Manager Extension** screen appears similar to the one shown below, right. Enter the appropriate extension, typically the same extension as the **Primary Handle** of the user account. This Communication Manager Extension must also be created on Communication Manager as described in **Section 4.6**.

#### Add User

|                                     |   |
|-------------------------------------|---|
| Primary Handle*                     | <input type="text" value="2003"/>         |
| User ID                             | <input type="text"/>                      |
| Password*                           | <input type="password" value="•••••"/>    |
| Confirm Password*                   | <input type="password" value="•••••"/>    |
| Host*                               | <input type="text" value="10.64.21.112"/> |
| First Name*                         | <input type="text" value="JNPR-SRX210"/>  |
| Last Name*                          | <input type="text" value="User 1"/>       |
| Address 1                           | <input type="text"/>                      |
| Address 2                           | <input type="text"/>                      |
| Office                              | <input type="text"/>                      |
| City                                | <input type="text"/>                      |
| State                               | <input type="text"/>                      |
| Country                             | <input type="text"/>                      |
| Zip                                 | <input type="text"/>                      |
| Survivable Call Processor           | <input type="text" value="none"/>         |
| Add Communication Manager Extension | <input checked="" type="checkbox"/>       |

Fields marked \* are required.

**Add**

#### Add Communication Manager Extension

Add Communication Manager extension for user 2003.

|                              |                                   |
|------------------------------|-----------------------------------|
| Extension                    | <input type="text" value="2003"/> |
| Communication Manager Server | <input type="text" value="8300"/> |

Fields marked \* are required.

**Add**

### 5.3.2. Juniper SRX-210 FXS Analog Phone SIP User Account

Each Juniper SRX-210 FXS Analog Phone must be configured with a SIP user account on SES and an Extension on Communication Manager. The following screens illustrate the creation of an SES user account with a Communication Manager Extension for one of the FXS Analog Phones on the Juniper SRX-210 of the sample configuration. This Communication Manager Extension must also be created on Communication Manager as described in **Section 4.6**.

#### Add User

|                                     |   |
|-------------------------------------|---|
| Primary Handle*                     | <input type="text" value="2001"/>         |
| User ID                             | <input type="text"/>                      |
| Password*                           | <input type="password" value="•••••"/>    |
| Confirm Password*                   | <input type="password" value="•••••"/>    |
| Host*                               | <input type="text" value="10.64.21.112"/> |
| First Name*                         | <input type="text" value="JNPR-SRX210"/>  |
| Last Name*                          | <input type="text" value="FXS1"/>         |
| Address 1                           | <input type="text"/>                      |
| Address 2                           | <input type="text"/>                      |
| Office                              | <input type="text"/>                      |
| City                                | <input type="text"/>                      |
| State                               | <input type="text"/>                      |
| Country                             | <input type="text"/>                      |
| Zip                                 | <input type="text"/>                      |
| Survivable Call Processor           | <input type="text" value="none"/>         |
| Add Communication Manager Extension | <input checked="" type="checkbox"/>       |

Fields marked \* are required.

 Add

#### Add Communication Manager Extension

Add Communication Manager extension for user 2001.

|                              |                                   |
|------------------------------|-----------------------------------|
| Extension                    | <input type="text" value="2001"/> |
| Communication Manager Server | <input type="text" value="8300"/> |

Fields marked \* are required.

 Add

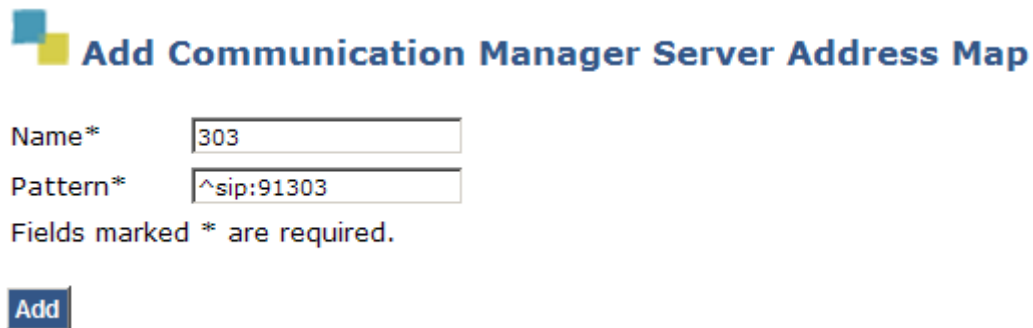
### 5.4. Communication Manager Address Maps

For incoming calls, SES uses Communication Manager address maps to direct the incoming SIP messages to the appropriate Communication Manager. SES directed all incoming calls to the 303 and 732 area codes to the Communication Manager for further routing in the sample configuration. Communication Manager routed 303 and 732 calls out its local PSTN trunk.

Communication Manager Address Maps are created by selecting **Communication Manager Servers → List** from the SES left navigation panel and then clicking the **Map** link.

Select **Add Another Map** in the resulting screen to add a map to an existing group or **Add Map In New Group** to create a map in a new group (not shown).

The screen below shows the map created for calls to the 303 area code.



**Add Communication Manager Server Address Map**

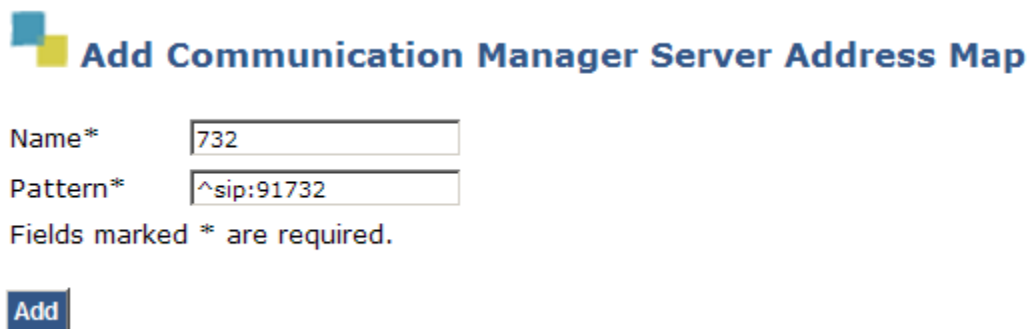
Name\*

Pattern\*

Fields marked \* are required.

**Add**

The screen below shows the map created for calls to the 732 area code.



**Add Communication Manager Server Address Map**

Name\*

Pattern\*

Fields marked \* are required.

**Add**

The List Communication Manager Server Address Map screen is shown below after the two mapped have been created.





## 6. Configure Avaya 9600 SIP Phones

The Avaya 9600 SIP Phones at all sites will use the SIP Enablement Services (10.64.21.112) as the SIP Proxy Server. The Avaya 9620 SIP Phones at the branch sites will also configure the on-site SRX210 (10.64.27.1) as an additional call server for survivability. The table below shows an example of the SIP telephone configuration settings for the Headquarters and the branch.

|                            | Headquarters  | Sample Branch |
|----------------------------|---------------|---------------|
| Extension                  | 1001          | 2003          |
| IP Address (DHCP)          | 10.64.21.116  | 10.64.27.102  |
| Subnet Mask                | 255.255.255.0 | 255.255.255.0 |
| Router                     | 10.64.21.1    | 10.64.27.1    |
| File Server                | 10.64.21.200  | 10.64.21.200  |
| SIP Domain                 | ses.avaya.com | ses.avaya.com |
| SIP Proxy Server           | 10.64.21.112  | 10.64.21.112  |
| Alternate SIP Proxy Server |               | 10.64.27.1    |

**Note:** The alternate SIP Proxy Server can be configured manually on the Avaya 9600 SIP Phones or through the 46xxsettings configuration file.

The configuration parameters of the Avaya 9600 SIP Phone specific to SIP Survivability in the 46xxsettings file are listed in the table below. See reference [5] for more details.

| 46xxsettings.txt<br>Parameter Name | Value Used in<br>Sample<br>Configuration                     | Description  |
|------------------------------------|--|--|
| <b>SIP_CONTROLLER_LIST</b>         | 10.64.21.112:5060;transport=tcp,<br>10.64.27.1;transport=udp | <p>A priority list of SIP Servers for the phone to use for SIP services. The port and transport use the default values of 5061 and TLS when not specified.</p> <p>The setting used in the sample configuration shows the values used for this parameter for a phone in the sample branch. The SIP Enablement Services is the first priority SIP Server listed using port 5060 and TCP transport. Separated by a comma, the sample branch Juniper SRX210 is the next priority SIP Server using port 5060 and UDP transport.</p> <p>The SIP Server list for each branch would require different values for</p> |

| 46xxsettings.txt<br>Parameter Name | Value Used in<br>Sample<br>Configuration | Description   |
|------------------------------------|--|---|
|                                    |  | the SIP_CONTROLLER_LIST, e.g. the list for Branch 1 phones will include the SIP Enablement Services and the Branch 1 Juniper SRX210 while the list for Branch 2 phones will include the SIP Enablement Services and the Branch 2 Juniper SRX210. To accomplish this, the GROUP system value mechanism can be implemented as described in [5].   |
| <b>FAILBACK_POLICY</b>             | Auto                                     | While in Survivable Mode, determines the mechanism to use to fail back to the centralized SIP Server.<br><b>Auto</b> = the phone periodically checks the availability of the primary controller and dynamically fails back.   |
| <b>FAST_RESPONSE_TIMEOUT</b>       | 2  | The timer terminates SIP INVITE transactions if no SIP response is received within the specified number of seconds after sending the request. Useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss.<br>The default value of 4 seconds may be retained if desired.<br>After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode. |
| <b>MSGNUM</b>                      | 1000                                     | The number dialed when the Message button is pressed and the phone is in Normal Mode.   |
| <b>PSTN_VM_NUM</b>                 | 913035383501                             | The number dialed when the Message button is pressed and the phone is in Survivable Mode.   |
| <b>RECOVERYREGISTERWAIT</b>        | 60                                       | A Reactive Monitoring Interval. If  |

| 46xxsettings.txt<br>Parameter Name | Value Used in<br>Sample<br>Configuration | Description   |
|------------------------------------|--|---|
|                                    |  | no response to a "maintenance check" REGISTER request is received within the timeout period, the phone will retry the monitoring attempt after a randomly selected delay of 50% - 90% of this parameter.  |
| <b>DISCOVER_AVAYA_ENVIRONMENT</b>  | 1  | Automatically determines if the active SIP Server is an Avaya server or not.  |
| <b>SIPREGPROXYPOLICY</b>           | simultaneous                             | A policy to control how the phone treats a list of proxies in the SIP_CONTROLLER_LIST parameter<br><b>alternate</b> = remain registered with only the active controller<br><b>simultaneous</b> = remain registered with all available controllers |
| <b>SIPDOMAIN</b>                   | ses.avaya.com                            | The enterprise SIP domain. Must be the same for all SIP controllers in the configuration. SIPDOMAIN is set to "avaya.com" in the sample configuration.  |

## 7. Configure Juniper SRX210

This section shows the configuration of the Juniper SRX210 Services Gateway to provide connectivity to a remote centralized SIP Peer-Call-Server (in this case a SIP Enablement Services server) which is providing call routing and handling for the branch during normal operations. It also shows the Branch SRX Survivable-Call-Server configuration providing local call handling and call routing when the SIP Enablement Services at the central site is no longer reachable.

The procedures described in this section include configurations in the following areas. It is assumed that the basic configuration of the Juniper SRX210 has already been administered. See references [6] and [7] for additional information.

- Verify POE and DHCP configuration
- Configuring Class of Restriction and Station Templates
- Configuring Analog and SIP Stations
- Configuring SRX Peer-call-Server
- Configuring Trunks and Trunk Groups
- Configuring Dial Plan for Normal Mode
- Configuring Media Gateway
- Configuring Dial Plan for Survivable Mode
- Configuring ICS Survivable Call Server
- Configuring Voice Mail Forwarding and Remote Access

The Juniper SRX210 configurations are performed through configuration CLI (Command Line Interface) commands in a terminal session using either of the following 2 access methods:

- Connect a PC to the branch SRX210 console port using a serial connection, then start a terminal session using Windows HyperTerminal
- Establish an SSH session to the SRX210.

Once a communications session is properly established, log in with administrative credentials, and then enter the configuration mode as shown below. The configuration commands shown in the ensuing sections are all issued from the CLI configuration mode.

```
--- JUNOS 10.1-20100504.0 built 2010-05-04 07:37:00 UTC
```

```
root@% cli
root> edit
Entering configuration mode

[edit]
root# _
```

## 7.1. Verifying POE and DHCP Configuration

DHCP is used to provide IP Addresses and configuration for the branch IP Phones. If POE and DHCP are already configured, this step may be skipped.

Use the following commands to enable POE and verify DHCP Services on a Branch SRX210. Note that the DHCP IP address ranges were previously administered for the sample configuration. Note that the sample configuration used the IP address space 10.64.27.0/24 only for voice communications; the IP address space 10.64.26.0/24 was set up for data communications and was not used in the sample configuration.

### Optional: Configure DHCP Options for BOOTP Server and Filename:

If the DHCP Provisioning method is used, you may need to specify option 242 for Avaya 9600-Series IP Phones. Setting option 242 string HTTPSRVR=10.64.21.200,L2QVLAN=0 tells the phones within the specified DHCP pool to connect to the HTTP Server at 10.64.21.200 to download configuration information and firmware:

```
[edit]
root# set poe interface all

root# edit system services dhcp
```

Under **[edit system services dhcp]**, issue following commands:

```
set option 242 string "HTTPSRVR=10.64.21.200,L2QVLAN=0"
```

## 7.2. Configuring Class of Restriction and Station Templates

A Class of Restriction policy is required before making any calls. The COR statements specify types of calls and whether or not they're allowed. If a policy allows a certain type of call and the Class of Restriction (COR) configuration that it belongs to is assigned to a station (or to a template that is assigned to a station), a user of the station's telephone is allowed to place the call. If a policy denies the call type, the user cannot make the call. By default, emergency and intra-branch calls do not require a Class of Restriction. In the sample configuration, any call type is configured to be allowed.

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set class-of-restriction cor1 policy 1 call-type any-call
set class-of-restriction cor1 policy 1 permission allow
```

A station template is a set of values configured to apply to stations of the same kind. Station templates for SIP and analog phones contain different parameters. Values configured for a station template are inherited by all stations it is applied to.

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set station-template sip-template SIPT dtmf-method rfc-2833
set station-template sip-template SIPT class-of-restriction corl
set station-template sip-template SIPT codec G711-MU

set station-template analog-template Analog class-of-restriction corl
```

### 7.3. Configuring Analog and SIP Stations

Analog stations connect to FXS interfaces on the branch SRX210. The branch SRX210 will register these stations to the SIP Enablement Services using the auth-id and auth-passwords specified. The station extension used here should have also been configured on the Communication Manager and the SIP Enablement Services as described in **Section 4.6** and **Section 5.3**. Configure the analog stations and apply the station-template “Analog” (created in **Section 7.2**) as follows:

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set station 2001 extension 2001
set station 2001 caller-id 2001
set station 2001 auth-id 2001 auth-password 123456
set station 2001 station-type analog template Analog
set station 2001 station-type analog tdm-interface fxs-0/0/10

set station 2002 extension 2002
set station 2002 caller-id 2002
set station 2002 auth-id 2002 auth-password 123456
set station 2002 station-type analog template Analog
set station 2002 station-type analog tdm-interface fxs-0/0/11
```

When the branch SRX210 is in Survivable Mode, local SIP phones will register to it. If authentication is desired, configure the branch SIP stations with an auth-id and auth-password. Configure the SIP stations and apply the station-template “SIPT” (created in **Section 7.2**) as follows:

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set station 2003 extension 2003
set station 2003 caller-id 2003
set station 2003 station-type sip template SIPT
```



```
set station 2003 auth-password 123456

set station 2004 extension 2004
set station 2004 caller-id 2004
set station 2004 station-type sip template SIPT
set station 2004 auth-password 123456
```

## 7.4. Configuring the SRX Peer-Call-Server

The branch SRX210 uses the SIP Enablement Services at the Headquarters to provide call handling and call routing services for all directly attached analog (FXS) and SIP endpoints in Normal Mode. This is accomplished by configuring the Peer-Call-Server on the branch SRX210. Below is the configuration of the Peer-Call-Server named “AvayaSM” as used during compliance testing.

```
[edit]
root# edit services converged-services
```

Under **[edit system services converged-services]**, issue following commands:

```
set peer-call-server AvayaSM address ipv4-addr 10.64.21.112
set peer-call-server AvayaSM codec G711-MU
set peer-call-server AvayaSM dtmf-method rfc-2833
set peer-call-server AvayaSM auth-id 2003
```

## 7.5. Configuring Trunks and Trunk Groups

The SRX210 dial plan includes route patterns that have one or more trunk groups. Each trunk group specifies one or more trunks to be used to route calls that specify a trunk's prefix, referred to as a trunk access code. To route calls to the PSTN from the branch, the branch SRX210 uses PSTN trunks for which interfaces are configured. The following commands illustrate how to configure two FXO trunks named "fxo12" and "fxo13" for PSTN access.

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set trunk fxo12 trunk-type fxo tdm-interface fxo-0/0/12
set trunk fxo13 trunk-type fxo tdm-interface fxo-0/0/13
```

Trunk groups combine trunks to be used to route calls. Add one or more trunks to a trunk group in the order they will be used. In the sample configuration, one trunk group named "MyTrunkGroup" was configured for PSTN and emergency calls.

```
[edit]
root# edit services converged-services

[edit services converged-services]
set trunk-group MyTrunkGroup trunk fxo12 trunk fxo13
```

**Note:** The SRX210 also supports a connection to a SIP trunk provided by a Service Provider. A SIP trunk can replace branch PSTN lines with a SIP trunking service from a Service Provider for branch calls to the PSTN. In the sample configuration, no direct SIP trunk to the Service Provider was configured. See **Section 1.1.5** for PSTN trunking configurations used in the sample configuration. The Distributed Trunking arrangement provides cost savings by routing local PSTN calls through the branch SRX210 FXO interfaces and long-distance toll calls via the T1/E1 facilities at the central site through the Avaya G-Series Media Gateway.

## 7.6. Configuring Dial Plan for Normal Mode

A dial plan for the Normal Mode must be configured to specify where calls will be routed. Route patterns of a dial plan include digit patterns against which called numbers are matched. Configure the dial plan for the Normal Mode when the Peer-Call-Server (the SIP Enablement Services at the central site) is in control.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set digit-manipulation digit-transform del-9 regular-expression "s/^9/"

set dial-plan plan2 route-pattern 9911 call-type trunk-call
set dial-plan plan2 route-pattern 9911 trunk-group MyTrunkGroup digit-
transform del-9

set dial-plan plan2 route-pattern 91732XXXXXXX call-type trunk-call digit-
transform del-9

set dial-plan plan2 route-pattern 91732XXXXXXX trunk-group MyTrunkGroup
```

911 from the branch will be sent back by the SIP Enablement Services server to the SRX210 and then be routed out to the PSTN through the “MyTrunkGroup” trunk group as configured in **Section 7.5**.

Note: For the branch phones to dial out to the PSTN, “9” must be dialed first before the actual dialed digits (as consistent with the Normal Mode dialing). The flexibility to not dial the “9” first may or may not be desirable in real deployments, and therefore should be modified as appropriate. If dialing a 9 is not required, use of the digit-manipulation rules and digit-transform options on the dial-plan are not required. In those cases the following dial-plan may be used.

```
set dial-plan plan2 route-pattern 911 call-type trunk-call
set dial-plan plan2 route-pattern 911 trunk-group MyTrunkGroup
set dial-plan plan2 route-pattern 1XXXXXXXXXX call-type trunk-call
set dial-plan plan2 route-pattern 1XXXXXXXXXX trunk-group MyTrunkGroup
```

## 7.7. Configuring Media Gateway

The Media Gateway must be configured for handling calls routed back from the SIP Enablement Services to the Branch SRX210. The Media Gateway “MGW”, as configured below, is bound to the peer-call-server “AvayaSM” and requires a dial-plan as configured in **Section 7.6**. The dial-plan associated with the Media Gateway is active whenever the Peer-Call-Server is reachable.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set media-gateway MGW peer-call-server AvayaSM
```

```
set media-gateway MGW dial-plan plan2
set media-gateway MGW protocol sip port 5060
set media-gateway MGW protocol sip transport udp
```

## 7.8. Configuring Dial Plan for Survivable Mode

When the SRX210 is in Survivable Mode, a separate call routing dial plan is put into use. In the Normally Mode, the SRX210 relies on the SIP Enablement Services at the central site to route calls, but when it is unreachable the SRX210 takes control and the dial plan for the Survivable Mode becomes active. The dial plan for the Survivable Mode may emulate the Peer-Call-Server dial plan (“plan2” in the sample configuration) so users will have a seamless experience (e.g. using the same dialed digits).

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

Set digit-manipulation digit-transform del-9 regular-expression "s/^9//"

set dial-plan plan1 route-pattern 911 call-type emergency-call
set dial-plan plan1 route-pattern 911 trunk-group MyTrunkGroup

set dial-plan plan1 route-pattern 91303XXXXXXX call-type long-distance-
call digit-transform del-9

set dial-plan plan1 route-pattern 91303XXXXXXX trunk-group MyTrunkGroup
digit-transform del-9

set dial-plan plan1 route-pattern 91732XXXXXXX call-type local-call digit-
transform del-9

set dial-plan plan1 route-pattern 91732XXXXXXX trunk-group MyTrunkGroup

set dial-plan plan1 route-pattern 9911 call-type emergency-call
set dial-plan plan1 route-pattern 9911 trunk-group MyTrunkGroup digit-
transform del-9
```

**Note:** With the sample configuration above, calls to the PSTN with area codes “732” and “303” from the branch are allowed. In real deployments, the dial-plan may be modified in accordance with appropriate business policies.

**Note:** For the branch phones to dial out to the PSTN, “9” must be dialed first before the actual dialed digits (as consistent with the Normal Mode dialing). The flexibility to not dial the “9” first may or may not be desirable in real deployments, and therefore should be modified as appropriate. If dialing a 9 is not required, use of the digit-manipulation rules and digit-transform options on the dial-plan are not required. In those cases the following dial-plan may be used.

```
set dial-plan plan2 route-pattern 911 call-type emergency-call
set dial-plan plan2 route-pattern 911 trunk-group MyTrunkGroup
```

```
set dial-plan plan2 route-pattern 1XXXXXXXXX call-type long-distance-call
set dial-plan plan2 route-pattern 1XXXXXXXXX trunk-group MyTrunkGroup
```

## 7.9. Configuring Survivable-Call-Server

When the Peer-Call-Server (SIP Enablement Services) is not available, the Survivable-Call-Server (SCS) on the SRX210 activates to provide call routing and handling services within the branch for analog FXS and local SIP phones. The following SCS configuration named “SCS” allows the SRX210 SCS to monitor the health of the Peer-Call-Server and provide call handling and routing when the Peer-Call-Server is unreachable. The dial-plan for the Survivable Mode must be associated with the SCS.

```
[edit]
root# edit services converged-services
```

Under **[edit services converged-services]**, issue following commands:

```
set survivable-call-service SCS peer-call-server AvayaSM
set survivable-call-service SCS dial-plan plan1
set survivable-call-service SCS registration-expiry-timeout 3600
```

## 7.10. Configuring Voice Mail Remote Access

In the Survivable Mode, the SRX210 covers unanswered calls at branch phones to the following PSTN remote access number of the voice mail messaging system if the call is not answered by the 4<sup>th</sup> ring.

```
[edit]
root# edit services converged-services
[edit services converged-services]
root# set features voicemail extension 1000 remote-access-number
913035383501
```

# 8. General Test Approach and Test Results

This section describes the validation test used to verify the sample configuration for the SIP Enablement Services Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in the branch. This section covers the general test approach and the test results.

## 8.1. General Test Approach

The general test approach was to break and restore network connectivity from the branch site to the Headquarters site to verify that

- When network connectivity is broken, the branch Juniper SRX210 gateway automatically assumes the SIP proxy and SIP registrar functions. In this Survivable Mode, the branch phones can still call each other and reach PSTN through the Juniper SRX210 FXO analog trunk interface.
- When network connectivity is restored, the SIP Enablement Services at the Headquarters location automatically assumes the SIP proxy and SIP registrar functions for providing

centralized SIP call control. In this Normal Mode, PSTN access by phones at both the headquarters and branch sites are through the T1/E1 connection on the Avaya Media Gateway at the central location.

## 8.2. Test Results

The following features and functionality were verified. Any observations related to these tests are listed at the end of this section:

- In Normal Mode, the SIP Enablement Services located at the central site serves as the SIP registrar and proxy for phones at both the central and branch sites; in Survivable Mode, the Juniper SRX210 located at the branch location serves as the SIP registrar and proxy for the branch phones.
- Branch phones register to the SIP Enablement Services and the branch Juniper SRX210 simultaneously. Switching between the Normal and the Survivable Modes is automatic and within a reasonable time span (within about 1 minute).
- In Normal Mode, calls can be placed between phones at the main site and the branch site, and among phones within the site.
- In Normal Mode, local and long-distance calls from the branch phones are routed to the PSTN through the T1/E1 connection on the Avaya Media Gateway at the central location.
- In Survivable Mode, calls can be placed among phones within the branch. In addition, branch phones can still place calls to the PSTN (and to the phones at Headquarters via PSTN) using the FXO interface on the branch Juniper SRX210.
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference on Avaya 9600 SIP Phones in both Normal and Survivable Modes.
- Analog phones connected to the FXS ports on the Juniper SRX210 are properly adapted as SIP phones in both Normal and Survivable Modes.
- Messaging system access by branch phones (through internal access number in Normal Mode and PSTN call in Survivable Mode) and proper function of MWI (Messaging Waiting Indicator) on the Avaya 9600 IP Phones in the Normal Mode.
- Proper system recovery after Juniper SRX210 restart and loss/restoration of IP connection.

The following problems were observed during compliance testing with disposition notes from Juniper (the JUNOS release in the notes refers to the Juniper SRX Services Gateway firmware):

1. There is no Music-On-Hold for the branch phones in the Survivable Mode.  
**Note:** Juniper reports this problem has been fixed with JUNOS release 10.2 R2.
2. There is no SRX configuration to control the number of rings before a call goes to coverage through FXO in the Survivable Mode.  
**Note:** Juniper reports this problem has been fixed with JUNOS release 10.2 R2.

The following functions/capabilities are currently unsupported by the Juniper SRX Services Gateway firmware (with notes made by Juniper):

- Normal Mode: Music-On-Hold (MoH) when the branch FXS phone calls branch and Headquarters endpoints and places the call on hold<sup>1</sup>.  
**Note:** The FXS ports on SRX210 do not support any supplementary services, including Hold; therefore, MoH is not an expected behavior.
- Alpha-numeric Caller-ID in the Survivable Mode.  
**Note:** The SRX currently supports numeric digit Caller-ID, but not alpha-numeric. This can be an enhancement per customer request.
- Call waiting using switch-hook flash to switch between calls on FXS-connected analog phones.  
**Note:** The FXS ports on SRX210 do not support any supplementary services, including switch-hook flash.
- Message Waiting Indicator (MWI) on branch IP phones and stutter-tone on branch FXS-connected analog phones for message waiting alert in the Survivable Mode.  
**Note:** MWI received by SIP phones prior to outage will keep blinking during outage. Stutter tone for analog phones can be an enhancement per customer request.
- The SRX210 does not respond properly to the SIP Options messages. The SRX210 responds with a “404 Not Found” rather than with a “200 OK”.  
**Note:** This can be an enhancement per customer request.
- Survivable Mode: Entire conference terminates when the conference initiating phone drops from the conference first  
**Note:** SRX implements 3-way calling in the Survivable Mode by having the handset mix the calls. This 3-way call model was tested with a variety of industry phones to work as designed. However, this call model differs from Avaya’s call conference model. Juniper is to offer a solution similar to Avaya’s call conference model where this caveat becomes critical.

---

<sup>1</sup> In the compliance tested configuration, the FXS phone Hold function is a function on the Avaya analog phone itself. It is not a capability on the SRX210.

## 9. Verification Steps

### 9.1. SRX210 Survivable-Call-Service State

The survivable-call-service state of the Juniper SRX210 can be verified by a CLI (Command Line Interface) command. Connect a PC to the SRX210 console port using a serial connection, and then start a terminal session using Windows HyperTerminal. The commands to type and the command output are shown in the screen below.

#### Normal Mode:

In Normal Mode, the “State” will be “Normal State” as shown in the first output line below.

#### Survivable Mode:

Before entering the same command again, the WAN cable was pulled out. The second output line shows “State” as “Survivable state”.

```
root>
root>
root>
root>
root>
root>
root>
root>
root> ... services convergence-services survivable-call-service sessions
Name          Address          Port            State
AvayaSM        10.64.21.112     UDP:5060        Normal state

root> ... services convergence-services survivable-call-service sessions
Name          Address          Port            State
AvayaSM        10.64.21.112     UDP:5060        Survivable state

root> _
```



## 9.2. Registered Peers on SRX210

The following screen shows registered peers (including SIP Enablement Services, branch FXS-connected analog phones, and SIP Phones) on the SRX210:

```
root>
root>
root>
root> show services convergence-services sip peers
Name/username      Host          Dyn Nat ACL Port      Status
AvayaSM/2003        10.64.21.112          5060      Unmonitored
2004/2004           10.64.27.101    D          5060      Unmonitored
2003/2003           10.64.27.102    D          5060      Unmonitored
2002-pcs/2002       10.64.21.112          5060      Unmonitored
2001-pcs/2001       10.64.21.112          5060      Unmonitored
5 sip peers [Monitored: 0 online, 0 offline Unmonitored: 5 online, 0 offline]
usp_ipc_process_destroy: destroyed usp ipc process
root> _
```

### **9.3. Verify Basic Calls**

In the Normal Mode, make calls between the Headquarters and the branch; verify that the calls are successful with a two-way talk-path. Make calls between the PSTN and the branch through the Headquarters; verify that the calls are successful with a two-way talk-path.

In the Survivable Mode, make calls between the branch phones; verify that the calls are successful with a two-way talk-path. Make calls between the PSTN and the branch through the FXO interfaces on the SRX210; verify that the calls are successful with a two-way talk-path

## **10. Conclusion**

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the centralized SIP call control platform occurs. Connectivity loss can be caused by WAN access problems being experienced at the branch or network problems at the centralized site blocking access to the Avaya SIP call control platform. These Application Notes present the configuration steps to implement the Avaya Aura<sup>TM</sup> SIP Enablement Services Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway to minimize service disruption impact to the remote branch SIP endpoints.

## 11. Additional References

The following Avaya documentation is available at: <http://support.avaya.com>.

### **Avaya Aura™ SIP Enablement Services 5.2.x:**

[1] *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-603323, February 2007.

[2] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May 2009.

[3] *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, Doc ID 03-600768, November 2009.

### **Avaya Aura™ Communication Manager 5.2.x:**

[4] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009.

### **Avaya one-X Deskphone Edition 9600 Series SIP IP Telephones (SIP 2.5.x):**

[5] *Avaya one-X Deskphone Edition for 9600 SIP IP Telephones Administrator Guide Release 2.5*, Doc ID 16-601944, November 2009.

The following Juniper documentation can be found at:

<http://www.juniper.net/techpubs/hardware/junos-srx/srx210/index.html>.

### **Juniper SRX210 Services Gateway:**

[6] *SRX 210 Hardware Guide*, Revision 02, May 2010.

[7] *SRX210 Documentation*, May 2010.

---

**©2010 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).